

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-312402

(43)Date of publication of application : 09.11.2001

(51)Int.Cl.

G06F 9/06
G06F 9/445
G06K 17/00
G06K 19/07
G06K 19/00

(21)Application number : 2000-129056

(71)Applicant : NTT DATA CORP

(22)Date of filing : 28.04.2000

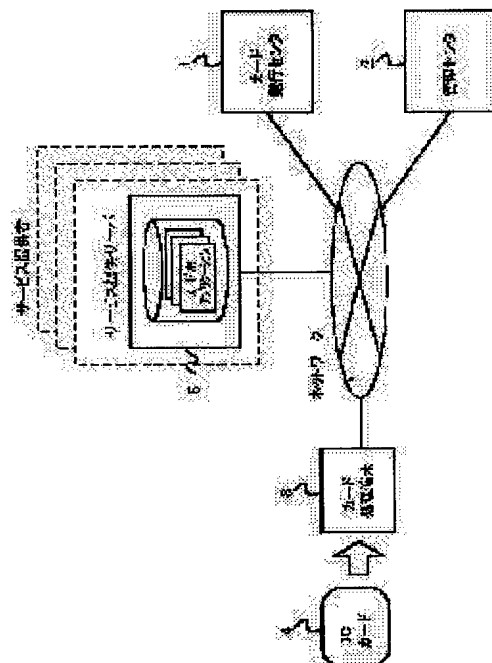
(72)Inventor : YAMAZAKI KENJI
SAKAI TAKAAKI
AMAMIYA SHUNICHI
TAMAI JUN
TOMINAGA HIROSHI
TAKAGI SOICHIRO

(54) CARD SYSTEM, IC CARD, AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a card system, etc., which can safely supply an application.

SOLUTION: An IC card 4 stores a permission table where the hash value of an application allowed by a card issue center 1 to be supplied is set. The IC card 4 obtains the hash value of an application supplied from a service providing server 5, decides whether the hash value matches the hash value registered in the permission table, and stores the application in a prescribed area of the IC card 4 when they match each other, but performs prescribed error processing when not.



LEGAL STATUS

[Date of request for examination]

04.04.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2001-312402
(P2001-312402A)

(43)公開日 平成13年11月9日(2001.11.9)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
G 0 6 F 9/06	5 5 0	G 0 6 F 9/06	5 5 0 G 5 B 0 3 5
9/445		G 0 6 K 17/00	B 5 B 0 5 8
G 0 6 K 17/00			D 5 B 0 7 6
19/07		G 0 6 F 9/06	4 2 0 J
		G 0 6 K 19/00	N
審査請求 未請求 請求項の数12 O L (全 14 頁) 最終頁に続く			

(21)出願番号 特願2000-129056(P2000-129056)

(22)出願日 平成12年4月28日(2000.4.28)

(71)出願人 000102728

株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号

(72)発明者 山崎 研史

東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内

(72)発明者 酒井 敬明

東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内

(74)代理人 100095407

弁理士 木村 満

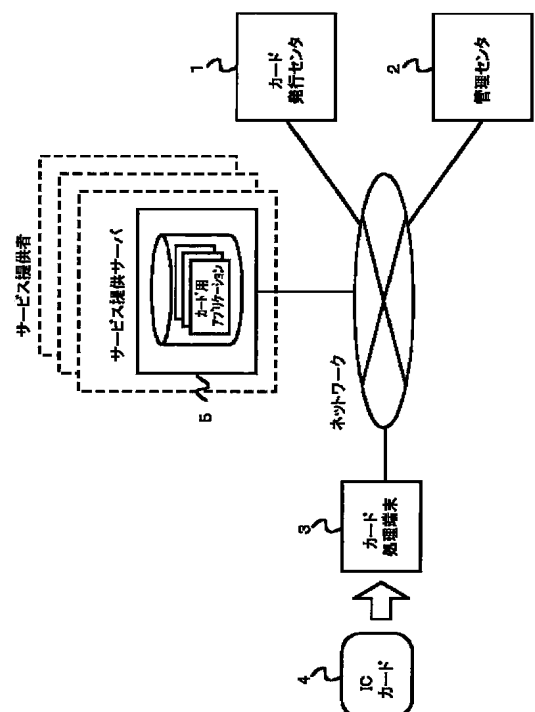
最終頁に続く

(54)【発明の名称】 カードシステム、ICカード及び記録媒体

(57)【要約】

【課題】 アプリケーションの供給を安全に行うことができるカードシステム等を提供する。

【解決手段】 ICカード4は、カード発行センタ1により供給が許可されたアプリケーションのハッシュ値が設定されている許可テーブルを記憶する。ICカード4は、サービス提供サーバ5から供給されたアプリケーションについてハッシュ値を求め、許可テーブルに登録されているハッシュ値と合致するか否かを判別し、合致する場合、そのアプリケーションをICカード4の所定領域に記憶し、合致しない場合、所定のエラー処理を行う。



(2)

1

【特許請求の範囲】

【請求項1】カード発行センタにより発行されたICカードに、供給センタにより供給されるアプリケーションを記憶するカードシステムであって、

前記ICカードは、

前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶し、

前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別し、

前記アプリケーションが前記許可テーブルに登録されている場合、該アプリケーションを当該ICカードの所定領域に記憶し、

前記アプリケーションが前記許可テーブルに登録されていない場合、所定のエラー処理を行う、

ことを特徴とするカードシステム。

【請求項2】前記許可テーブルには、各前記アプリケーションについて、当該アプリケーションに基づいて導出されるチェック情報がそれぞれ設定され、

前記ICカードは、

前記供給センタからのアプリケーションの供給に応答し、前記供給されたアプリケーションに基づいてチェック情報を導出し、前記許可テーブルに設定されている該

該当するアプリケーションのチェック情報と照合し、

前記チェック情報が合致する場合には、前記供給されたアプリケーションを当該ICカードの所定領域に記憶し、

前記チェック情報が合致しない場合には、所定のエラー処理を行う、

ことを特徴とする請求項1に記載のカードシステム。

【請求項3】前記チェック情報はハッシュ値を含む、ことを特徴とする請求項2に記載のカードシステム。

【請求項4】前記許可テーブルには、管理機関による署名が付与されている、

ことを特徴とする請求項1又は2に記載のカードシステム。

【請求項5】カード発行センタにより発行されたICカードに、供給センタにより供給されるアプリケーションを記憶するカードシステム用のICカードであって、

前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶し、

前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別し、

前記アプリケーションが前記許可テーブルに登録されている場合、該アプリケーションを当該ICカードの所定領域に記憶し、

前記アプリケーションが前記許可テーブルに登録されていない場合、所定のエラー処理を行う、

ことを特徴とするICカード。

【請求項6】カード発行センタにより発行されたICカードに、供給センタにより供給されるアプリケーション

2

を記憶するカードシステムであって、

前記供給センタは、前記カード発行センタから認証情報を取得し、取得した前記認証情報とアプリケーションを前記ICカードに供給し、

前記ICカードは、前記供給センタからの前記認証情報の正当性をチェックし、チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該IC

カードの所定領域に記憶し、チェック結果がエラーを示す場合、所定のエラー処理を行う、

ことを特徴とするカードシステム。

【請求項7】前記供給センタは、ICカードにアプリケーションを供給するとき、アプリケーションの供給先のICカードからカード識別符号を取得し、取得した前記カード識別符号とアプリケーション識別符号を前記カード発行センタに供給し、

前記カード発行センタは、前記アプリケーション識別符号に基づくアプリケーションに関する情報を、前記カード識別符号により特定されるICカードの鍵で暗号化したものを前記認証情報として前記供給センタに供給し、

前記ICカードは、当該ICカードの鍵を用いて前記認証情報の正当性をチェックする、

ことを特徴とする請求項6に記載のカードシステム。

【請求項8】供給センタは、ICカードにアプリケーションを供給するとき、アプリケーションの供給先のICカードから乱数を取得し、取得した乱数とアプリケーション識別符号を前記カード発行センタに供給し、

前記カード発行センタは、前記乱数と前記アプリケーション識別符号に基づくアプリケーションに関する情報を当該カード発行センタの鍵で暗号化したものを前記認証

情報として前記供給センタに供給し、

前記ICカードは、乱数を生成して前記供給センタに供給し、前記供給センタから供給された前記認証情報の正当性を前記カード発行センタの鍵を用いてチェックする、

ことを特徴とする請求項6に記載のカードシステム。

【請求項9】前記ICカードは、当該ICカードに記憶されているアプリケーションの削除に伴い、削除対象のアプリケーションに関する削除証明書を作成し、前記削除対象のアプリケーションの供給元の供給センタに供給し、

前記供給センタは、前記ICカードからの削除証明書を前記カード発行センタに送信する、

ことを特徴とする請求項6乃至8のいずれか1項に記載のカードシステム。

【請求項10】カード発行センタにより発行されたICカードに、供給センタにより供給されるアプリケーションを記憶するカードシステム用のICカードであって、

前記ICカードは、前記供給センタが前記カード発行センタから取得した認証情報を受け取って、該認証情報の正当性をチェックし、チェック結果が正常を示す場合、

前記供給センタは、前記ICカードからの削除証明書を前記カード発行センタに送信する、

ことを特徴とする請求項6乃至8のいずれか1項に記載のカードシステム。

【請求項11】カード発行センタにより発行されたICカードに、供給センタにより供給されるアプリケーションを記憶するカードシステム用のICカードであって、

前記ICカードは、前記供給センタが前記カード発行センタから取得した認証情報を受け取って、該認証情報の正当性をチェックし、チェック結果が正常を示す場合、

50

(3)

3

前記供給センタからのアプリケーションを当該 IC カードの所定領域に記憶し、チェック結果がエラーを示す場合、所定のエラー処理を行う、ことを特徴とする IC カード。

【請求項 11】コンピュータを、カード発行センタにより発行され、供給センタにより供給されるアプリケーションを記憶する IC カードとして機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

該コンピュータを、

前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶する手段、

前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別する手段、

前記判別手段により前記アプリケーションが前記許可テーブルに登録されていると判別された場合、該アプリケーションを当該 IC カードの所定領域に記憶する手段、前記判別手段により前記アプリケーションが前記許可テーブルに登録されていないと判別された場合、所定のエラー処理を行う手段、

として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 12】コンピュータを、カード発行センタにより発行され、供給センタにより供給されるアプリケーションを記憶する IC カードとして機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

該コンピュータを、

前記供給センタが前記カード発行センタから取得した認証情報を受け取る手段、

前記認証情報の正当性をチェックする手段、

前記チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該 IC カードの所定領域に記憶する手段、

前記チェック結果がエラーを示す場合、所定のエラー処理を行う手段、

として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、カード発行センタにより発行された IC カードに、アプリケーションの供給を行う供給センタにより供給されるアプリケーションを記憶するカードシステム等に関する。

【0002】

【従来の技術】例えばカード発行者が各利用者に対して発行した IC カードに、アプリケーションの供給者（サービス提供者）がカード用アプリケーションを供給して、IC カードの多目的利用を図るカードシステムが知られている。このようなシステムでは、例えば、利用者

4

は所望のアプリケーションを自己の IC カードにダウンロードし、IC カードに組み込まれたアプリケーションを実行させることにより、サービス提供者による所定のサービスを受けることができる。

【0003】

【発明が解決しようとする課題】上記のようなカードシステムでは、例えば不正なサービス提供者による IC カードへのアプリケーションの供給を防止し、安全にアプリケーションの供給が受けられる仕組みが必要とされている。

【0004】また、システムの安全性を保持する観点からアプリケーションの供給者（サービス提供者）の認証処理を行う場合、その認証処理が複雑化・長時間化してしまうと、システムのレスポンスを低下させてしまうおそれがある。

【0005】また、カード発行者により各 IC カードへのアプリケーションの供給状況が正確に把握され、例えば各サービス提供者への適正な課金管理が実現されること等が業界において望まれている。

【0006】本発明は、上述した事情に鑑みてなされたもので、アプリケーションの供給を安全に行うことができるカードシステム等を提供することを目的とする。また、本発明は、アプリケーションの供給者の認証処理の複雑化・長時間化を防止することができるカードシステム等を提供することを他の目的とする。また、本発明は、IC カードへのカード用アプリケーションの登録状況の管理が可能なシステム等を提供することを他の目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するため、本発明の第 1 の観点に係るカードシステムは、カード発行センタにより発行された IC カードに、供給センタにより供給されるアプリケーションを記憶するカードシステムであって、前記 IC カードは、前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶し、前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別し、前記アプリケーションが前記許可テーブルに登録されている場合、該アプリケーションを当該 IC カードの所定領域に記憶し、前記アプリケーションが前記許可テーブルに登録されていない場合、所定のエラー処理を行う。

【0008】このような構成によれば、IC カードに予めカード発行センタが許可したアプリケーションに関する許可テーブルを格納しておき、IC カードにアプリケーションをダウンロードする際に、そのアプリケーションの正当性を許可テーブルを参照してチェックする。これにより、ダウンロードする度にカード発行センタにアプリケーションの正当性を問い合わせることなく、カード内でその正当性をチェックすることができるため、安

(4)

5

全性が高く、短時間で認証が可能なカードシステムを実現することができる。

【0009】前記許可テーブルには、各前記アプリケーションについて、当該アプリケーションに基づいて導出されるチェック情報がそれぞれ設定されてもよく、前記ICカードは、前記供給センタからのアプリケーションの供給に応答し、前記供給されたアプリケーションに基づいてチェック情報を導出し、前記許可テーブルに設定されている該当するアプリケーションのチェック情報と照合してもよく、前記チェック情報が合致する場合には、
10 前記供給されたアプリケーションを当該ICカードの所定領域に記憶してもよく、前記チェック情報が合致しない場合には、所定のエラー処理を行ってもよい。

【0010】前記チェック情報はハッシュ値を含んでもよい。

【0011】前記許可テーブルには、管理機関による署名が付与されていてもよい。これにより、許可テーブルを用いてアプリケーションのチェックを行うことは、カード発行センタと管理機関の両方からの許可を確認することと実質的に同意となるため、さらにシステムの安全性を高めることができる。また、第三者的な管理機関による署名を付与することで、例えばカード発行元とアプリケーション供給者（サービス提供者）の共同による不正行為等を防止することができる。

【0012】また、本発明の第2の観点に係るICカードは、カード発行センタにより発行されたICカードに、供給センタにより供給されるアプリケーションを記憶するカードシステム用のICカードであって、前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶し、前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別し、前記アプリケーションが前記許可テーブルに登録されている場合、該アプリケーションを当該ICカードの所定領域に記憶し、前記アプリケーションが前記許可テーブルに登録されていない場合、所定のエラー処理を行う、ことを特徴とする。

【0013】また、本発明の第3の観点に係るカードシステムは、カード発行センタにより発行されたICカードに、供給センタにより供給されるアプリケーションを記憶するカードシステムであって、前記供給センタは、前記カード発行センタから認証情報を取得し、取得した前記認証情報とアプリケーションを前記ICカードに供給し、前記ICカードは、前記供給センタからの前記認証情報の正当性をチェックし、チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該ICカードの所定領域に記憶し、チェック結果がエラーを示す場合、所定のエラー処理を行う、ことを特徴とする。

【0014】このような構成によれば、ICカードにアプリケーションを供給する時にはカード発行センタによ

6

り発行される認証情報が必要とされる。これにより、カード発行センタから認証情報を取得していないサービス提供サーバによるICカードへのアプリケーションの登録を排除し、安全なカードシステムを提供することができる。

【0015】前記供給センタは、ICカードにアプリケーションを供給するとき、アプリケーションの供給先のICカードからカード識別符号を取得し、取得した前記カード識別符号とアプリケーション識別符号を前記カード発行センタに供給してもよく、前記カード発行センタは、前記アプリケーション識別符号に基づくアプリケーションに関する情報を、前記カード識別符号により特定されるICカードの鍵で暗号化したものを前記認証情報として前記供給センタに供給してもよく、前記ICカードは、当該ICカードの鍵を用いて前記認証情報の正当性をチェックしてもよい。

【0016】また、供給センタは、ICカードにアプリケーションを供給するとき、アプリケーションの供給先のICカードから乱数を取得し、取得した乱数とアプリケーション識別符号を前記カード発行センタに供給してもよく、前記カード発行センタは、前記乱数と前記アプリケーション識別符号に基づくアプリケーションに関する情報を当該カード発行センタの鍵で暗号化したものを前記認証情報として前記供給センタに供給してもよく、前記ICカードは、乱数を生成して前記供給センタに供給し、前記供給センタから供給された前記認証情報の正当性を前記カード発行センタの鍵を用いてチェックしてもよい。

【0017】前記ICカードは、当該ICカードに記憶されているアプリケーションの削除に伴い、削除対象のアプリケーションに関する削除証明書を作成し、前記削除対象のアプリケーションの供給元の供給センタに供給してもよく、前記供給センタは、前記ICカードからの削除証明書を前記カード発行センタに送信してもよい。

【0018】これにより、アプリケーションがICカードに供給される度に供給センタがカード発行センタから認証情報を取得するため、カード発行センタは、各ICカードへアプリケーションが供給されたことを確実に把握することができる。また、ICカードがアプリケーションの削除についての証明書を供給センタに対して発行し、供給センタがその証明書をカード発行センタに提出することにより、カード発行センタは、各ICカードからアプリケーションが削除されたことを確実に把握することができる。また、カード発行センタは、各ICカードについて、アプリケーションの登録及び削除を確実に把握できるため、供給センタに対して適正な課金管理を行うことができる。

【0019】また、本発明の第4の観点に係るICカードは、カード発行センタにより発行されたICカードに、供給センタにより供給されるアプリケーションを記

50

(5)

7

憶するカードシステム用の IC カードであって、前記 IC カードは、前記供給センタが前記カード発行センタから取得した認証情報を受け取って、該認証情報の正当性をチェックし、チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該 IC カードの所定領域に記憶し、チェック結果がエラーを示す場合、所定のエラー処理を行う、ことを特徴とする。

【0020】また、本発明の第5の観点に係る記録媒体は、コンピュータを、カード発行センタにより発行され、供給センタにより供給されるアプリケーションを記憶する IC カードとして機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、該コンピュータを、前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶する手段、前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別する手段、前記判別手段により前記アプリケーションが前記許可テーブルに登録されていると判別された場合、該アプリケーションを当該 IC カードの所定領域に記憶する手段、前記判別手段により前記アプリケーションが前記許可テーブルに登録されていないと判別された場合、所定のエラー処理を行う手段、として機能させるためのプログラムを記録する。

【0021】また、本発明の第6の観点に係る記録媒体は、コンピュータを、カード発行センタにより発行され、供給センタにより供給されるアプリケーションを記憶する IC カードとして機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、該コンピュータを前記供給センタが前記カード発行センタから取得した認証情報を受け取る手段、前記認証情報の正当性をチェックする手段、前記チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該 IC カードの所定領域に記憶する手段、前記チェック結果がエラーを示す場合、所定のエラー処理を行う手段、として機能させるためのプログラムを記録する。

【0022】

【発明の実施の形態】以下、本発明の実施の形態に係るカードシステムを図面を参照して説明する。このカードシステムは、カード発行者が利用者に対して発行した IC カードに、アプリケーションの供給者（サービス提供者）により供給される種々のカード用アプリケーションをダウンロードして組み込むためのものである。

【0023】（第1の実施形態）本発明の第1の実施形態に係るカードシステムのシステム構成図を図1に示す。図示されるように、このカードシステムは、カード発行センタ1と、管理センタ2と、カード処理端末3と、IC カード4と、各サービス提供者のサービス提供サーバ5と、を備える。

【0024】カード発行センタ1は、利用者に対する IC

8

C カード3の発行等を行う。この IC カード3の発行では、カード発行センタ1は、各サービス提供サーバ5が配信するカード用アプリケーションに基づいて、カード用アプリケーションに関する所定のテーブル（許可テーブル）を作成し、その許可テーブルに対して管理センタ2から署名の付与を受ける。そして、署名が付与された許可テーブルと所定のカード情報（カードID等）を発行対象の IC カード3に記録して発行する。

【0025】カード発行センタ1により生成される許可テーブルには、例えば図2に示すように、各サービス提供サーバ5が提供するカード用アプリケーションについて、アプリケーションID、ハッシュ値等の情報が、サービス提供サーバ5を識別するためのサービス提供者ID毎に設定される。このハッシュ値は、例えばカード用アプリケーションのプログラム等、カード用アプリケーション毎に一意の情報に基づいて生成される。

【0026】管理センタ2は、カード発行センタ1からの要求に応じて、カード発行センタ1が生成した許可テーブルに対して署名（管理者署名）を付与する。

【0027】カード処理端末3は、IC カードリーダ／ライタ等を備え、主に IC カード4とサービス提供サーバ5との間のデータ送受信等を行う。例えば、カード処理端末3は、利用者から入力されたカード用アプリケーションのダウンロードの要求をカードリーダ／ライタを介して IC カード4に通知し、これに応じて IC カード4から受信したカードID等をカード用アプリケーションのダウンロード要求とともにサービス提供サーバ5に送信する。また、サービス提供サーバ5から受信したカード用アプリケーションをカードリーダ／ライタを介して IC カード4に送信等する。

【0028】IC カード4は、MPU、ROM、RAM、EEPROM等を有する IC チップを備え、この IC チップは、例えば図3に示すように、MPUがROM等に記憶されるプログラムを実行することにより実現される制御部41とメモリ42と入出力制御部43とを備える。

【0029】制御部41は、カード処理端末3からの所定の通知に応じて、メモリに記憶されるカードID等をカード処理端末3に送信する。そして、制御部41は、ダウンロードされたカード用アプリケーションをカード処理端末3から受信すると、そのカード用アプリケーションのハッシュ値を作成する。そして、受信したカード用アプリケーションのアプリケーションIDと、作成したハッシュ値を、メモリ42に記憶されている許可テーブルの設定値と照合する。

【0030】比較したアプリケーションID及びハッシュ値が一致する場合には、制御部41は、そのカード用アプリケーションが予めカード発行センタ1に許可されたものであるとして、メモリ42におけるカード用アプリケーションを記憶するための記憶領域に、受信したカ

(6)

9

ード用アプリケーションを記憶する。

【0031】また、比較したアプリケーションID及びハッシュ値が一致しない場合には、制御部41は、カード発行センタ1が許可したカード用アプリケーションでないと判別し、カード用アプリケーションを所定の記憶領域に記憶することなく、カード処理端末3にエラー信号を送信して、エラー表示させる等の所定のエラー処理を行う。

【0032】メモリ42は、許可テーブル、カード情報（カードID等）、カード用アプリケーション等を記憶する。入出力制御部43は、カード処理端末3とのデータ通信を制御する。

【0033】サービス提供サーバ5は、ICカード4へのカード用アプリケーションの提供等を行うためのサーバである。サービス提供サーバ5は、カード処理端末3からのカード用アプリケーションのダウンロード要求に応答して、該当するカード用アプリケーションを図示せぬ記憶部から読み出して、要求元のカード処理端末3に送信する。

【0034】次に、この第1の実施形態に係るシステムにおいて、ICカード4にカード用アプリケーションを登録する場合の処理を図4を参照して説明する。例えば、ある利用者は、カード処理端末3にICカード4をセットして、サービス提供サーバ5（サービス提供者ID：BBB）が提供するカード用アプリケーション（アプリケーションID：123）のダウンロード要求を入力する。これに応じて、カード処理端末3はダウンロードの要求の入力をICカード4に通知して、カードID等を取得し、アプリケーションID「123」のカード用アプリケーションのダウンロード要求とともにサービス提供サーバ5に送信する（ステップS1、S2）。

【0035】ダウンロード要求を受信したサービス提供サーバ5は、該当するアプリケーションID「123」のカード用アプリケーションを読み出して、カード処理端末3を介してICカード4に送信する（ステップS3）。

【0036】ICカード4は、受信したカード用アプリケーションについてハッシュ値（例えば、「23」）を生成する（ステップS4）。そして、受信したカード用アプリケーションのアプリケーションID「123」と、生成したハッシュ値「23」が、メモリ42に記憶されているサービス提供者ID「BBB」の許可テーブルの設定値と合致するかを判別する（ステップS5）。

【0037】比較したアプリケーションID及びハッシュ値が合致する場合、ICカード4は受信したカード用アプリケーションを、カード発行センタ1から許可されている正当なアプリケーションであるとして、メモリ42のカード用アプリケーション用領域に格納する（ステップS6）。

【0038】また、例えば、比較したアプリケーション

10

IDとハッシュ値が許可テーブルの設定値と合致しない場合には、ICカード4は、受信したカード用アプリケーションを、カード発行センタ1からの許可を受けていない不当なアプリケーションであるとして、例えば、そのカード用アプリケーションをカード用アプリケーション用の記憶領域に記憶することなく消去して、カード処理端末3にエラー信号を送信する等の所定のエラー処理を実行する（ステップS7）。

【0039】このようにして、ICカード4に予めカード発行センタ1が許可したカード用アプリケーションに関する許可テーブルを格納しておき、ICカード4にカード用アプリケーションをダウンロードする際に、そのカード用アプリケーションの正当性を許可テーブルを参照してチェックする。これにより、ダウンロードする度にカード発行センタ1にカード用アプリケーションの正当性を問い合わせることなく、カード内でその正当性をチェックすることができるため、安全性が高く、短時間での認証が可能なカードシステムを実現することができる。

【0040】また、ICカード4に格納される許可テーブルには、管理センタ2による管理者としての署名が付与されているため、この許可テーブルを用いてカード用アプリケーションのチェックを行うことは、カード発行センタ1と管理センタ2の両方からの許可を確認することと実質的に同意である。よって、さらにシステムの安全性を高めることができる。また、第三者的な管理センタ2による署名を付与することで、例えばカード発行元とサービス提供者の共同による不正行為等を防止することができる。

【0041】また、管理センタ2を除いたシステム構成としてもよい。この場合、許可テーブルに第三者に管理センタ2による署名は付与されないが、上記説明のように、ICカード4内で許可テーブルに基づくチェックを行うため、安全性が高く、短時間での認証が可能なカードシステムを実現することができる。

【0042】また、各サービス提供者が提供するカード用アプリケーションが追加される場合や新たなサービス提供者が追加される場合等に、新たな許可テーブルをカード発行センタ1がカード処理端末3を介してICカード4に供給するようにしてもよい。

【0043】また、許可テーブルに記憶するチェック用データはハッシュ値に限定されない。例えば各カード用アプリケーションに対して一意な数値、データ等を導出できる任意の関数を用いてもよい。

【0044】また、サービス提供者のカード用アプリケーションを記憶部に格納し、カードリーダライタを備えるサービス提供装置を用いてもよい。この場合、利用者は、サービス提供装置にICカード4をセットして、所望のカード用アプリケーションのICカード4への書込要求を入力する。この入力に応じて、サービス提供装置

(7)

11

は、指定されたカード用アプリケーションを記憶部から読み出して、ICカード4に渡す。ICカード4は、上記説明と同様にして、許可テーブルに基づくカード用アプリケーションのチェックを行い、その正当性を確認した場合にはメモリ42の所定記憶領域に記録し、不当であると判別した場合には受け取ったアプリケーションを消去する等のエラー処理を行う。

【0045】（第2の実施形態）本発明の第2の実施形態に係るカードシステムのシステム構成図を図5に示す。図示されるように、このカードシステムは、カード発行センタ6と、カード処理端末7と、ICカード8と、各サービス提供者のサービス提供サーバ9と、を備える。

【0046】カード発行センタ6は、利用者に対するICカード8の発行等を行う。カード発行センタ6は、発行対象の各ICカード8のメモリに、カード毎に一意の暗号鍵（カード用秘密鍵）を記録する。また、カード発行センタ6は、例えば図6に示すような、各ICカード8のカードIDと暗号鍵（カード用公開鍵）を対応付ける鍵テーブルを記憶する。また、カード発行センタ6は、各サービス提供サーバ9が提供するカード用アプリケーションについて、アプリケーションIDと、そのカード用アプリケーションに基づいて生成されたハッシュ値が対応付けられているテーブルを記憶する。

【0047】カード発行センタ6は、サービス提供サーバ9から、例えばカードIDとサービス提供者IDとアプリケーションIDを含む鍵要求情報を受信すると、鍵要求情報に含まれるアプリケーションIDに対応するハッシュ値を読み出す。そして、鍵要求情報に含まれるカードIDに対応する暗号鍵（カード用公開鍵）を鍵テーブルから読み出し、その暗号鍵で先に取得したハッシュ値を暗号化し、暗号化されたハッシュ値に、カード発行センタ6による署名を付与して要求元のサービス提供サーバ9に送信する。

【0048】また、カード発行センタ6は、サービス提供サーバ9から受信した鍵要求情報に基づいて、例えば図7に示すような、サービス提供者ID、カードID、アプリケーションID、登録日時等を含む課金情報を生成して記憶する。そして、この課金情報に基づいて、ICカード8にカード用アプリケーションを供給するサービス提供者に対して課金を行う。課金の方法は任意であり、例えば、1アプリケーション毎に、カードへの記録時間が所定時間経過する毎に所定金額がアプリケーション提供元に課金されるようにしてもよい。

【0049】また、カード発行センタ6は、サービス提供サーバ9から、サービス提供者IDとアプリケーションの削除に関する証明書を受信すると、課金情報を参照して、受信データに該当する課金情報を特定し、その課金情報に対して、例えばアプリケーションの削除日時等の情報を設定する。なお、この証明書は、ICカード8

12

からカード用アプリケーションが削除された場合にICカード8によりサービス提供サーバ9に対して発行される情報であり、例えば、削除されたアプリケーションIDとカードID等を含む。この証明書は、例えばICカード8の秘密鍵で署名がなされていてもよい。この場合、カード発行センタ6は、ICカード8の公開鍵を用いて署名を確認することにより、証明書の正当性を確認する。

【0050】カード処理端末7は、ICカードリーダ／ライタ等を備え、主にICカード8とサービス提供サーバ9との間のデータ送受信等を行う。例えば、カード処理端末7は、利用者から入力されたカード用アプリケーションのダウンロード又は削除の要求等をカードリーダ／ライタを介してICカード8に通知し、これに応じてICカード8から受信したカードIDをカード用アプリケーションのダウンロード要求又は削除要求通知等とともにサービス提供サーバ9に送信する。また、カード処理端末7は、サービス提供サーバ9から受信したアクセス要求、暗号化されたハッシュ値、カード用アプリケーション等をカードリーダ／ライタを介してICカード4に送信する。

【0051】ICカード8は、MPU、ROM、RAM、EEPROM等を有するICチップを備え、このICチップは、例えば図8に示すように、MPUがROM等に記憶されるプログラムを実行することにより実現される制御部81とメモリ82と入出力制御部83とを備える。

【0052】制御部81は、カード処理端末7からの、ダウンロードの要求、カード用アプリケーションの削除の要求等が入力されたことの通知に応じて、メモリに記憶されるカードID等をカード処理端末7に送信する。

【0053】また、制御部81は、サービス提供サーバ9からの、ICカード8へのアクセス要求（書込要求）と暗号化されたハッシュ値とカード用アプリケーション等をカード処理端末7を介して受信すると、暗号化されたハッシュ値に付与されている署名の検証を行う。そして、署名が正しければ、メモリ82に記憶されている暗号鍵（カード用秘密鍵）を用いて、暗号化されたハッシュ値を復号化する。次に、復号化したハッシュ値を、受信したカード用アプリケーションに基づいて作成したハッシュ値と照合する。そして、比較したハッシュ値が一致する場合には、制御部81は、メモリ82におけるカード用アプリケーションを記憶するための記憶領域に、受信したカード用アプリケーションを記憶する。また、比較したハッシュ値が一致しない場合には、制御部81は、カード用アプリケーションを所定の記憶領域に記憶することなく、カード処理端末7にエラー信号を送信して、エラー表示させる等の所定のエラー処理を行う。

【0054】また、制御部81は、サービス提供サーバ9からの、カード用アプリケーションの削除要求等をカ

(8)

13

ード処理端末7を介して受信すると、指定されたカード用アプリケーションをメモリ82から削除する。そして、削除したカード用アプリケーションのアプリケーションID、そのICカード8のカードID等を含む証明書をカード処理端末7を介してサービス提供サーバ9に送信する。なお、この証明書にICカード8の秘密鍵を用いた署名を付与してもよい。

【0055】メモリ82は、暗号鍵（カード用秘密鍵）、カード発行者の公開鍵、カード情報（カードID等）、カード用アプリケーション等を記憶する。入出力制御部83は、カード処理端末7とのデータ通信を制御する。

【0056】サービス提供サーバ9は、ICカード8へのカード用アプリケーションの提供等を行うためのサーバである。サービス提供サーバ9は、カード処理端末7からの、カード用アプリケーションのダウンロード要求に回答して、例えば、ダウンロード要求とともに受信したカードIDと、要求されたカード用アプリケーションのアプリケーションIDと、サービス提供者IDを含む鍵要求情報を生成して、カード発行センタ6に送信し、暗号化されたハッシュ値をカード発行センタ6から受信する。そして、サービス提供サーバ9は、ダウンロード要求に該当するカード用アプリケーションを図示せぬ記憶部から読み出し、暗号化されたハッシュ値と所定のアクセス要求（書込要求）とともにカード処理端末7を介してICカード8に送信する。

【0057】また、サービス提供サーバ9は、カード処理端末7からのカード用アプリケーションの削除要求通知に回答して、指定されたアプリケーションの削除要求をカード処理端末7を介してICカード8に送信する。そして、ICカード8からの証明書をカード処理端末7を介して受信し、この証明書をカード発行センタ6に送信する。

【0058】次に、この第2の実施形態に係るシステムにおいて、ICカード8にカード用アプリケーションを登録する場合の処理を図9を参照して説明する。例えば、ある利用者は、カード処理端末7にICカード8

（カードID：3232）をセットして、サービス提供サーバ9が提供するカード用アプリケーションのダウンロード要求を入力する。これに応じて、カード処理端末7はダウンロードの要求の入力をICカード8に通知して、カードID「3232」等を取得し、カード用アプリケーションのダウンロード要求（ダウンロード対象のアプリケーションIDを含む）とともにサービス提供サーバ9に送信する（ステップS11、S12）。

【0059】ダウンロード要求を受信したサービス提供サーバ9は、受信したカードID「3232」と、要求されたカード用アプリケーションのアプリケーションIDと、サービス提供者IDを含む鍵要求情報を生成して、カード発行センタ6に送信する（ステップS1

14

3）。

【0060】カード発行センタ6は、鍵要求情報の受信に回答し、この受信データに含まれるアプリケーションIDに対応するハッシュ値を読み出す。また、カードID「3232」に対応する暗号鍵「1212」を鍵テーブルから読み出して、その暗号鍵でハッシュ値を暗号化し、暗号化されたハッシュ値にカード発行センタ6の秘密鍵を用いた署名を付与して要求元のサービス提供サーバ9に送信する（ステップS14）。また、カード発行センタ6は、サービス提供サーバ9からの受信データを用いて課金情報を生成して記憶する（ステップS15）。そして、課金情報に基づいてサービス提供者がカードID「3232」にカード用アプリケーションを提供することに対して課金を行う。

【0061】また、サービス提供サーバ9は、カード発行センタ6から受信した暗号化されたハッシュ値と、要求されたカード用アプリケーションと、アクセス要求（書込要求）を、カード処理端末7を介してICカード8に送信する（ステップS16）。

【0062】ICカード8は、受信した暗号化されたハッシュ値に付与されている署名について、カード発行センタの公開鍵を用いて検証する。署名が正しければ、暗号鍵（カード用秘密鍵）を用いて暗号化されたハッシュ値を復号化する。そして、復号化されたハッシュ値が、受信したカード用アプリケーションに基づいて作成したハッシュ値と合致するかを判別する（ステップS17）。

【0063】比較したハッシュ値が合致する場合、ICカード8は、送信元の正当性を確認したとして、受信したカード用アプリケーションを、メモリ82のカード用アプリケーション領域に格納する（ステップS18）。

【0064】また、比較したハッシュ値が合致しない場合又は署名が不当なものである場合等には、ICカード8は、例えば、そのカード用アプリケーションをカード用アプリケーション用の記憶領域に記憶することなく消去して、カード処理端末7にエラー信号を送信する等の所定のエラー処理を実行する（ステップS19）。

【0065】次に、この第2の実施形態に係るシステムにおいて、ICカード8からカード用アプリケーションを削除する場合の処理を図10を参照して説明する。例えば利用者は、カード処理端末7にICカード8（カードID：3232）をセットして、ICカード8に記憶されているカード用アプリケーションの削除要求を入力する。これに応じて、カード処理端末7はアプリケーションの削除の要求の入力をICカード8に通知して、カードID「3232」等を取得し、カード用アプリケーションの削除要求通知（削除対象のアプリケーションIDを含む）とともにサービス提供サーバ9に送信する（ステップS21、S22）。

(9)

15

【0066】削除要求を受信したサービス提供サーバ9は、指定されたカード用アプリケーションを削除するためのアクセス要求（削除要求）をカード処理端末7を介してICカード8に送信する（ステップS23）。これに応じて、ICカード8は、指定されたカード用アプリケーションをメモリ82から削除するとともに、このカード用アプリケーションを削除したことを示す証明書を作成する（ステップS24、S25）。そして、作成した証明書をカード処理端末7を介してサービス提供サーバ9に送信する（ステップS26）。

【0067】サービス提供サーバ9は、ICカード8から受信した証明書をカード発行センタ6に送信する（ステップS27）。カード発行センタ6は、受信した証明書からカード用アプリケーションが削除されたことを確認し、該当する課金情報にカード用アプリケーションの削除日時等を設定する（ステップS28）。

【0068】このようにして、ICカード8にカード用アプリケーションを登録する時には、カード用アプリケーションの情報をICカード8に固有の鍵で暗号化したものにカード発行センタ6が署名をしたものを必要とする。これにより、そのカードにしか有効でない認証用情報がカード発行センタ6により生成されるため、不正なサービス提供サーバ9によるICカード8へのカード用アプリケーションの登録を排除し、安全なカードシステムを提供することができる。また、ICカード8によりカード用アプリケーションの削除についての証明書を発行させて、サービス提供サーバ9にその証明書を提出させること等により、カード発行センタ6では、各ICカード8へのカード用アプリケーションに登録及び削除を確実に把握できるため、適正な課金管理を行うことができる。

【0069】また、ICカード8のカード用アプリケーションを削除する場合も、登録の場合と同様に、カード発行センタ6による認証を必要とするようにしてもよい。この場合、サービス提供サーバ9は、登録の場合と同様に、カード発行センタ6から暗号化されたハッシュ値と署名を取得して、カード用アプリケーションの削除要求とともに暗証鍵をICカード8に対して送信する。

【0070】また、サービス提供者のカード用アプリケーションを記憶部に格納し、カードリーダライタを備えるサービス提供装置を用いても良い。この場合、利用者は、サービス提供装置にICカード8をセットして、所望のカード用アプリケーションのICカード8への書込要求を入力する。この入力に応じて、サービス提供装置は、カードIDとアプリケーションIDをカード発行センタ6に送信して、これに対する暗号化されたハッシュ値と署名をカード発行センタ6から取得し、指定されたカード用アプリケーションとともにICカード8に渡す。ICカード8は、上記説明と同様にして、署名及びハッシュ値のチェックを行い、その正当性を確認した場

16

合にはメモリ82の所定記憶領域にカード用アプリケーションを記録し、不当であると判別した場合には受け取ったアプリケーションを消去する等のエラー処理を行う。

【0071】また、カード発行センタ6において、ICカード8の暗号鍵で暗号化するものはアプリケーションIDに対応するハッシュ値に限定されず、そのカード用アプリケーションに一意な情報であればよい。例えば、アプリケーションIDをICカード8の暗号鍵で暗号化したものに署名を付与して、サービス提供サーバ9に供給するようにしてもよい。この場合、ICカード8は、署名を検証した後、暗号化されたアプリケーションIDを暗号鍵で復号化し、受信したカード用アプリケーションのアプリケーションIDであるかを判別する。

【0072】また、カード用アプリケーションのICカード8への登録に先立ってICカード8が乱数を生成し、その乱数をカード発行センタ6による署名の対象に含めるようにしてもよい。この場合、例えば図11に示すように、サービス提供サーバ9は、ICカード8に対して、乱数の生成を要求する（ステップS31）。これに応じて、ICカード8は、乱数を生成し、生成した乱数等をサービス提供サーバ9に送信する（ステップS32）。サービス提供サーバ9は、受信した乱数等と、ダウンロード対象のカード用アプリケーションのアプリケーションID等をカード発行センタ6に送信する（ステップS33）。

【0073】これに応じて、カード発行センタ6は、受信したアプリケーションIDに対応するハッシュ値を読み出す。そして、読み出したハッシュ値と受信した乱数をカード発行センタ6の秘密鍵で暗号化した許可情報を生成し、要求元のサービス提供サーバ9に送信する（ステップS34）また、カード発行センタ6は、サービス提供者に対する課金を行う。サービス提供サーバ9は、カード発行センタ6から受信した許可情報と、要求されたカード用アプリケーションをアクセス要求とともにICカード8に送信する（ステップS35）。

【0074】ICカード8は、受信した許可情報をカード発行センタ6の公開鍵で復号化して、ハッシュ値と乱数を取得する。そして、取得した乱数を、自己が生成した乱数と照合する。また、ICカード8は、受信したカード用アプリケーションに基づいて作成した作成したハッシュ値を、受信したハッシュ値と照合する（ステップS36）。

【0075】そして、乱数の照合結果とハッシュ値の照合結果の双方が正常である場合には、受信したカード用アプリケーションをメモリ82の所定領域に格納し（ステップS37）、いずれかの照合結果がエラーを示す場合には、そのカード用アプリケーションを所定領域に記憶することなく消去して、カード処理端末7にエラー信号を送信する等の所定のエラー処理を行う（ステップS

(10)

17

38)。

【0076】このようにして、乱数を用いることにより、1回限り有効な認証用情報が作成されるため、セキュリティのレベルを高めることができる。また、この例においても、カード発行センタ6における暗号化の対象はアプリケーションIDに対応するハッシュ値に限定されず、そのカード用アプリケーションに一意な情報であればよい。例えば乱数とアプリケーションIDをカード発行センタ6に秘密鍵で暗号化したものを許可情報としてサービス提供サーバ9に供給するようにしてもよい。この場合、ICカード8は、復号化して得た乱数についての照合とアプリケーションIDについての照合を行う。

【0077】また、上記実施例において用いる暗号方式は秘密鍵暗号方式に限定されず、共通鍵暗号方式を用いてもよい。

【0078】また、第1と第2の実施の形態におけるカード処理端末3、7は、携帯端末（携帯電話機）等を含む。

【0079】なお、この発明のシステムは、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、コンピュータに上述の動作を実行させるためのプログラムを格納した媒体（フロッピー（登録商標）ディスク、CD-ROM等）から該プログラムをインストールすることにより、上述の処理を実行するカード発行センタ1、6、管理センタ2、カード処理端末2、7等を構成することができる。なお、上述の機能を、OSが分担又はOSとアプリケーションの共同により実現する場合等には、OS以外の部分のみを媒体に格納してもよい。

【0080】なお、搬送波にプログラムを重畳し、通信ネットワークを介して配信することも可能である。例えば、通信ネットワークの掲示板（BBS）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、OSの制御下で、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【0081】

【図2】

サービス提供者ID			
アプリケーションID	123	213	345
ハッシュ値	23	34	17
⋮	⋮	⋮	⋮

18

【発明の効果】以上説明したように、本発明によれば、カード発行センタによる認証を受けていない供給センタによるICカードへのアプリケーションの供給を排除し、安全なアプリケーションの供給を可能とする。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るカードシステムのシステム構成図である。

【図2】許可テーブルを説明するための図である。

【図3】図1のカードシステムで使用されるICカードの構成を説明するための図である。

【図4】図1のカードシステムにおいてICカードにカード用アプリケーションを登録する場合の処理を説明するための図である。

【図5】本発明の第2の実施形態に係るカードシステムのシステム構成図である。

【図6】鍵テーブルを説明するための図である。

【図7】課金情報を説明するための図である。

【図8】図5のカードシステムで使用されるICカードの構成を説明するための図である。

【図9】図5のカードシステムにおいてICカードにカード用アプリケーションを登録する場合の処理を説明するための図である。

【図10】図5のカードシステムにおいてICカードからカード用アプリケーションを削除する場合の処理を説明するための図である。

【図11】図5のカードシステムにおいてICカードにカード用アプリケーションを登録する場合の処理の他の例を説明するための図である。

【符号の説明】

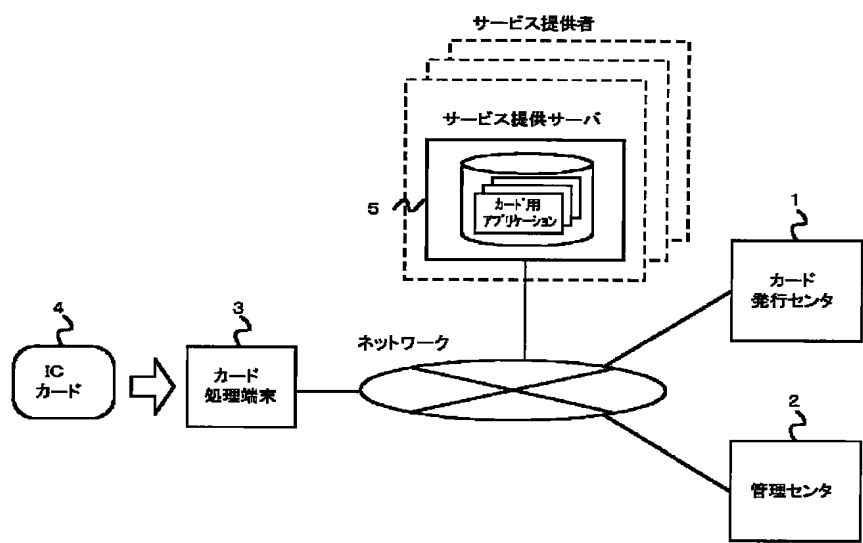
- 1、6 カード発行センタ
2 管理センタ
3、7 カード処理端末
4、8 ICカード
5、9 サービス提供サーバ
41、81 制御部
42、82 メモリ
43、83 入出力制御部

【図6】

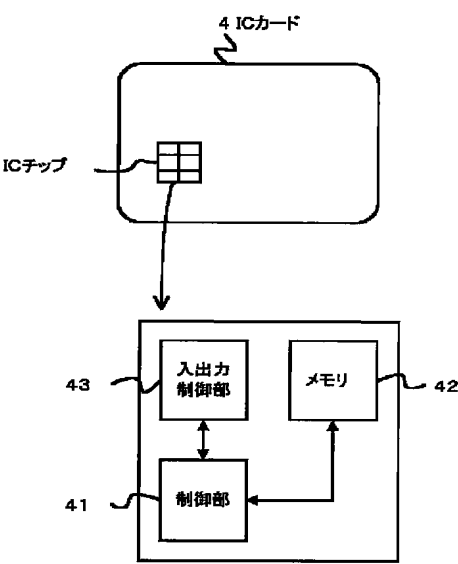
鍵テーブル	
カードID	暗証鍵
9876	XXXXXX
5432	XXXXXX
⋮	⋮

(11)

【図1】



【図3】

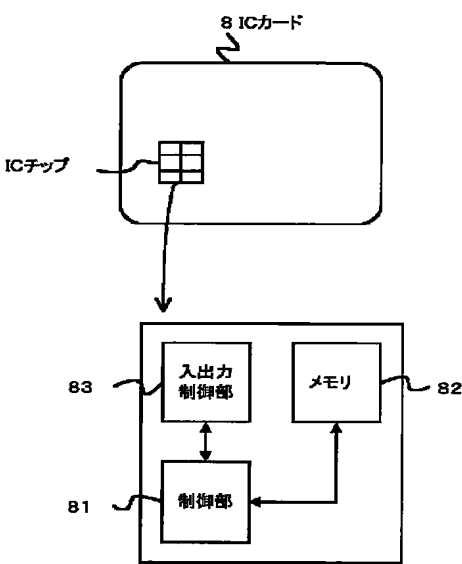


【図7】

課金テーブル

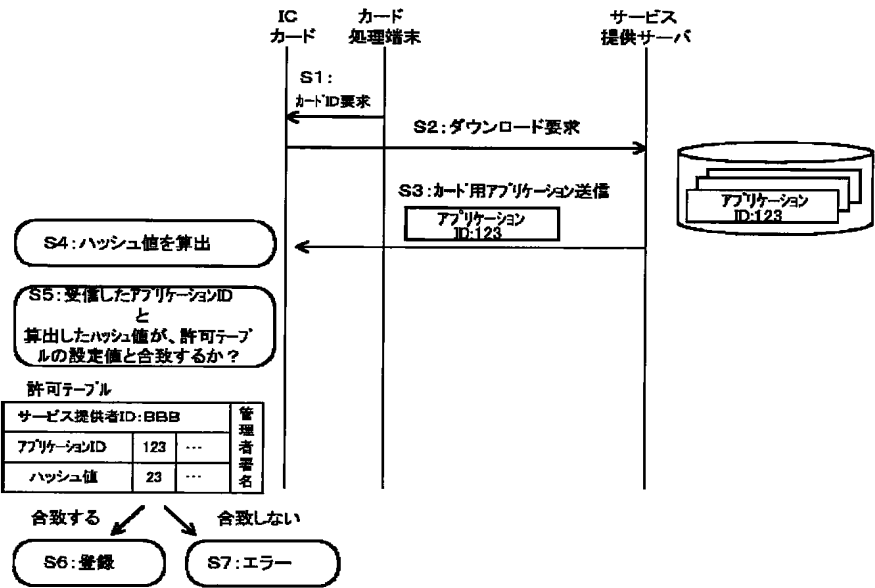
サービス提供者ID	カードID	アプリケーションID	登録日時	...
876	1234	111	XXXX/XX/XX XX:XX	...
432	5678	222	XXXX/XX/XX XX:XX	...
⋮	⋮	⋮	⋮	⋮

【図8】

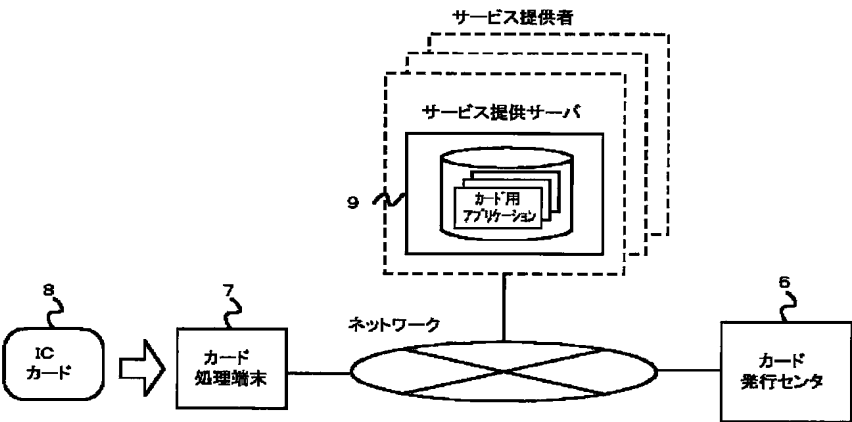


(12)

【図4】

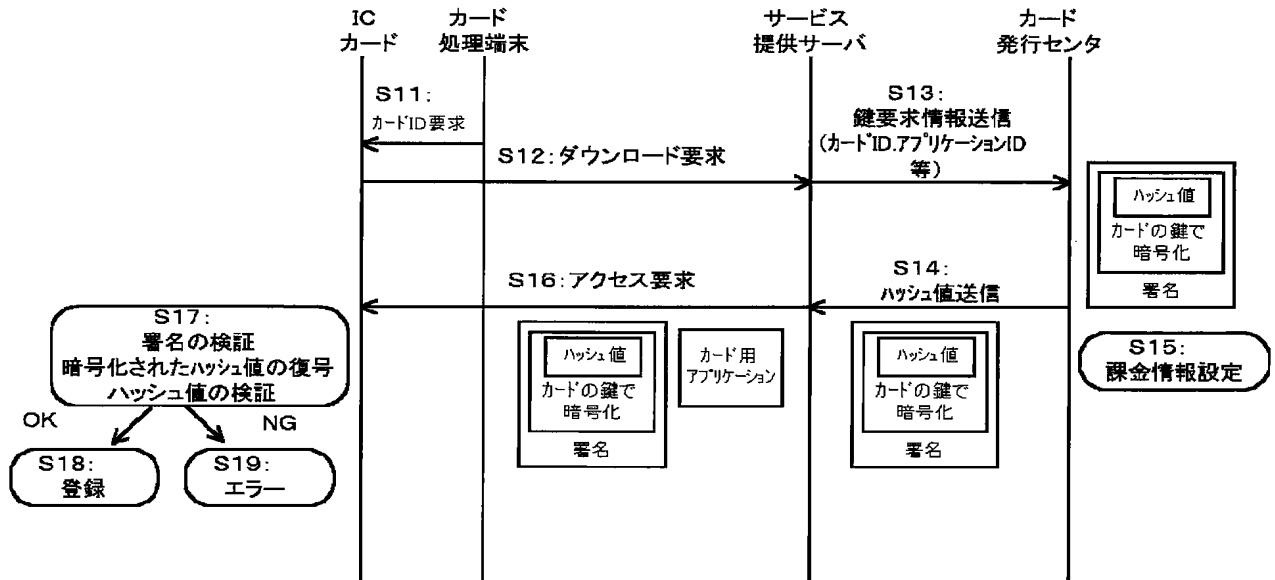


【図5】

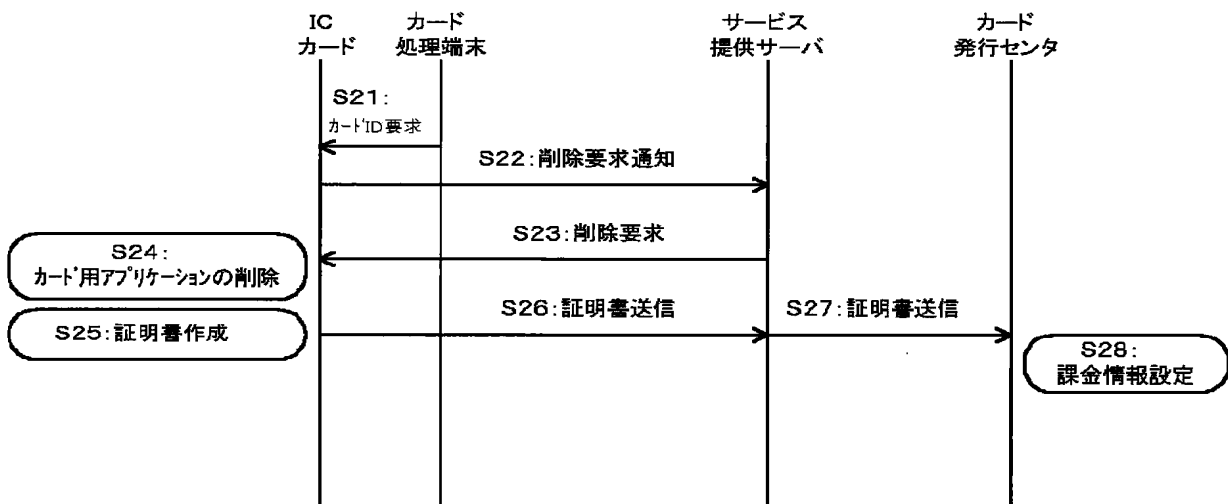


(13)

【図9】

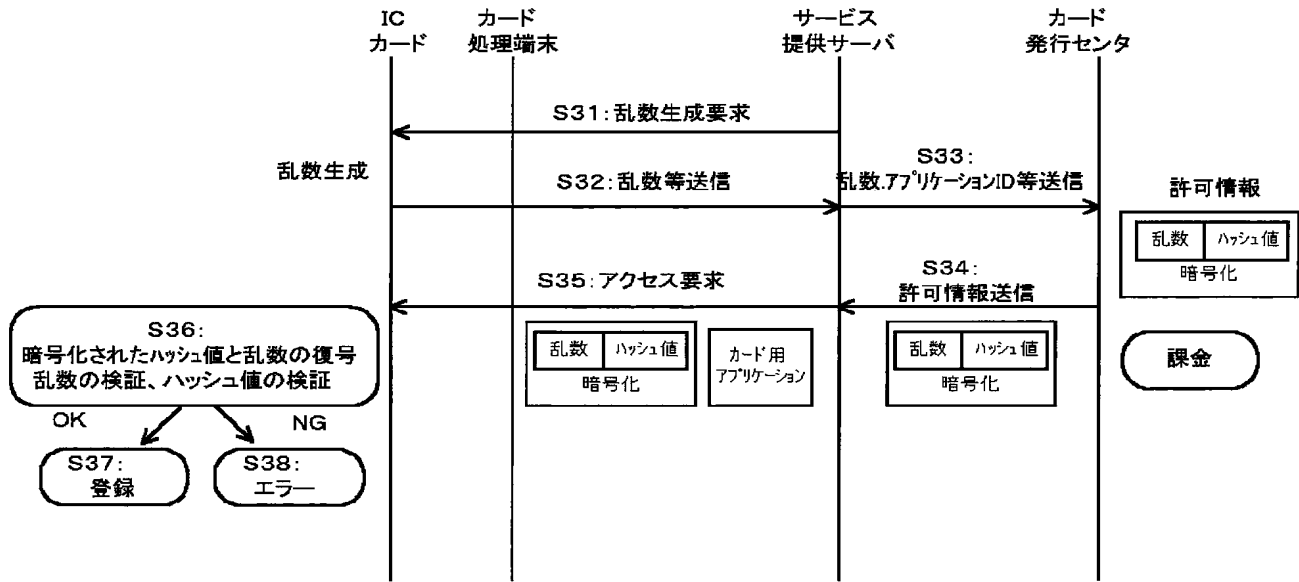


【図10】



(14)

【図 11】



フロントページの続き

(51) Int. Cl. ⁷ G 0 6 K 19/00	識別記号	F I G 0 6 K 19/00	テーマコード (参考) Q
(72) 発明者 雨宮 俊一 東京都江東区豊洲三丁目 3 番 3 号 株式会 社エヌ・ティ・ティ・データ内		(72) 発明者 富永 洋 東京都江東区豊洲三丁目 3 番 3 号 株式会 社エヌ・ティ・ティ・データ内	
(72) 発明者 玉井 純 東京都江東区豊洲三丁目 3 番 3 号 株式会 社エヌ・ティ・ティ・データ内		(72) 発明者 高木 聡一郎 東京都江東区豊洲三丁目 3 番 3 号 株式会 社エヌ・ティ・ティ・データ内	
		F ターム (参考) 5B035 AA06 AA13 BB09 CA29 5B058 KA11 KA31 KA33 5B076 BB06 FB02 FB09	